Norsk Kryptoseminar 2024

Slobodan Petrovic & Tjerand Silde @ Gjøvik

NTNU Gjøvik

Context and history of NKS

A yearly event open to everyone interested in cryptography, a meeting place for academia, industry, and public sector.

A long tradition that stopped for a few years but has recently been organized at Kjeller (2020), Trondheim (2021), Bergen (2022), Oslo (2023), and Gjøvik (2024). Next year: Oslo.

The agenda usually contains invited talks, updates on research, short talks by PhD students, and conversations.

Signal Group for NKS

NTNU

Program

1015: Opening
1030: Invited talks
- "Oppdaterte kryptografiske anbefalinger fra NSM" – Thomas Gregersen (NSM)
- "A demo of post-quantum TLS on an Android device" – Ella Kristensen (Thales Norway)

1200: Lunch
1300: Invited talks
- "eIDAS: Digital Identity today and in the future" – Mads Henriksveen (Buypass)
- "Machine learning in the encrypted domain - what can be done in practice?" – Håvard Raddum (Simula UiB)

1430: Updates from research institutions
- NSM – Espen Auseth Nielsen
- FFI – Martin Strand
- Simula UiB – Martijn Stam
- UiB – Nikolay Kaleyski
- UiO – Håkon Jacobsen
- NTNU – Tjerand Silde

1500: PhD candidate presentations
- "Private set intersection from key exchange" – Emil August Hovd Olaisen (NTNU)
- "Glitch Detectors and How They Can Fail" – Amund Askeland (NSM/UiB)
- "Federated Secure Messaging" – Hagen Echzell (UiO)
- "PQC acceleration for safety-critical applications" – Mohamed Abdelmonem (Simula UiB)
- "Long lasting privacy for e-voting" – Oskar Goldhahn (NTNU)
- "Cryptographically optimal functions" – Nadiia Ichanska (UiB)

1630: Wrap up

NTNU

WELCOME!